United Nations A/60/95/Add.1

General Assembly

Distr.: General
21 September 2005

Original: English

Sixtieth session
Agenda item 86
Developments in the field of information and telecommunications in the context of international security

Developments in the field of information and telecommunications in the context of international security

Report of the Secretary-General

Addendum

Contents

Page

II. Replies received from Governments 2
Brazil 2
Canada 4

05-51877 (E) 111005

II. Replies received from Governments

Brazil

[Original: English]
[24 June 2005]

In analysing the impact of developments in information and telecommunication technology upon international security, one must begin by acknowledging that the relationship between societies and technological development cannot be described by simple, one-way interactions; it hinges upon a complex interaction among necessities, creativity, entrepreneurial initiatives and the collective utilization of technology. The twenty-first century is the dawn of a new era, during which the rise of the "information society" is expected to determine deep transformations in all areas of human activity, from individual and societal interactions to patterns of economic production and State governance.

Information has already become a crucial element for the wealth and prosperity of nations, and is rightly considered today one of their most valuable resources. Private companies, banks, stock markets and governmental organizations (including defence establishments) are all interconnected by worldwide information networks, which have become as vital for economic progress as electric power and water supply. However, this high and ever-increasing degree of connectivity also creates a new set of potential vulnerabilities for Governments and economies, which may be exploited for use both in military conflicts and in criminal and terrorist activities.

In recent decades, the massive use of technology and automation in warfare has created the conditions for conflicts among States to be more focused in military objectives and to avoid collateral damage. At the same time, the growing influence of the media and of organized civil society imposes many constraints on the conduct of military operations. Contemporary warfare is supposed to be "clean" or even "surgical".

This fits well with the concrete possibilities offered by "cyberwarfare". Some armed forces are already deploying specialized military units, trained and equipped to disable or even destroy critical infrastructure by means of invasion and sabotage of information networks. Depending on the objective and the means employed, the effects of such attacks may range from "soft kills" of enemy weapon or sensor systems to cataclysmic disruptions of nationwide power grids. The efficiency of this form of warfare is increased by the fact that many of those capabilities may be constituted with comparatively small investments. In view of these factors, cyberwarfare may well become the stepping-stone of military interstate conflicts in the near future. The same vulnerabilities may also come to be exploited by terrorist organizations, with potentially even greater and more unpredictable negative consequences.

Albeit on a lesser scale in terms of magnitude of effects, such offensive information technology tools are already being widely used by criminals: every year, the information technology systems of numerous financial institutions, commercial enterprises and governmental agencies are hacked and invaded by individuals or groups unlawfully seeking profit and/or privileged information.

Aware of the importance of this subject for the maintenance of international peace and security, Brazil suggests that the issue be approached in two different ways. First, the international community should strive to build appropriate tools for dealing with criminal and terrorist activities involving information technology. In a separate but complementary approach, it should consider the impact of the emergence of cyberwarfare and the potential need for disarmament and non-proliferation regimes and international law concerning war to take into account its manifold effects.

Considering the possibility of terrorist and criminal actions, we suggest that the United Nations lead the Member States to establish, in cooperation, the following measures:

- Establish emergency and alternative networks to protect critical infrastructure
- Examine their network structure, analysing the interdependencies, and identify effective methods of protection
- Promote interactions between government and private sectors, aiming at reaching the desired level of security for the information that flows among organizations
- Establish protection systems to avoid or to minimize the effects of cyberattacks
- Implement tools and measures to enable authorities to trace the origin of cyberattacks
- Qualify national institutions to conduct testing and evaluation of the security level of information systems
- Negotiate and adopt an international convention on cybercrimes
- Promote and develop the technology regarding the means and methods of information security
- Guarantee access to the available information and information technology for the whole public
- Avoid establishing mechanisms that could prevent countries from accessing high technology in the field of telecommunications and information systems
- Create procedures for the mutual notification of cyberthreats among competent national authorities
- Educate the population about the importance of cybersecurity.

Concerning the use of information weapons in inter-State conflict, we believe that the United Nations should evaluate the possibility of promoting conventions regarding the following themes:

- Identification, characteristics and classification of information warfare
- Identification and classification of information weapons and means that can be used as information weapons
- Prevention of the use of cybernetic military weapons or knowledge by terrorist groups

- Establishment of a code of conduct for the use of information weapons
- Guarantee that all countries have equal rights regarding the protection of their homeland against cyberattacks
- Creation of international mechanisms in order to guide the solution of conflicts related to cybernetic aggressions
- Creation of a United Nations glossary containing definitions of main terms related to information security.

Canada

[Original: English]
[4 August 2005]

Information infrastructure is a key component of Canada's critical infrastructure, which includes the following sectors: energy and utilities, communications and information technology, finance, health care, food, water, transportation, Government and manufacturing. The challenges of securing the information infrastructure are the same across all sectors, of which up to 90 per cent is estimated to be owned and operated privately. The importance of Canada's information infrastructure to all Canadians has prompted the Government to work to maintain the security, availability and integrity of its systems, take steps in preventing cyberincidents and respond quickly to any reported disruptions.

In December 2003, the Prime Minister announced the creation of a new Department of Public Safety and Emergency Preparedness (PSEPC). This new government department brought the former Office of Critical Infrastructure Protection and Emergency Preparedness, the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS) — three main federal agencies with cybersecurity mandates — into the same Ministry. PSEPC is responsible for monitoring and analysing cyberthreats to government systems, providing a central reporting point for cyberincidents and alerting government departments to new threats and vulnerabilities. CSIS is responsible for investigating incidents posing a threat to national security. RCMP is responsible for investigating any criminal or potentially criminal cyberincidents. Additionally, the Communications Security Establishment is the information technology security technical authority responsible for developing operational standards for system certification and accreditation, risk and vulnerability analysis, product evaluation, system security and network security analysis.

In April 2004, Canada released its first National Security Policy, which sets out an integrated strategy and action plan designed to address current and future threats. This plan specifically confirmed that cybersecurity was a challenge in terms of public safety and proposed the establishment of a high-level national Cybersecurity Task Force with public and private representation to develop a national cybersecurity strategy to address this issue. The Task Force is in the process of being formed.

In February 2005, PSEPC created the Canadian Cyberincident Response Centre (CCIRC) to serve as a national focal point for coordinating cybersecurity incident response and monitoring the cyberthreat environment. CCIRC operates out

of the Government Operations Centre, a facility that runs 24 hours a day, 7 days a week, as part of Canada's National Emergency Response System.

Canadian provinces and territories are focusing on protecting their own critical infrastructures, including the cybersystems and networks on which they depend. Work is under way on interprovincial initiatives, such as a collaborative cybermonitoring capability.

The private sector is actively involved in cybersecurity initiatives. Private sector companies protect their own critical information technology infrastructures and, through industry associations, work to share information on cybervulnerabilities, incidents and solutions within their sectors. Industry associations work with PSEPC in a forum that permits a broad exchange on information across industry sectors.

Canada has also been involved in multilateral initiatives on cybersecurity. These include the Group of 8 Subgroup on High-tech Crime, which was established in 1997 and which adopted 10 principles to combat computer crime; the Council of Europe Convention on Cybercrime, which aims to harmonize national laws that define offences as well as define investigation and prosecution procedures to cope with global networks and establish a rapid and effective system of international cooperation; and the Organization of American States, whose Member States agreed "to consider the preparation of pertinent inter-American legal instruments and model legislation for the purpose of strengthening hemispheric cooperation in combating cybercrime considering standards relating to privacy, the protection of information, procedural aspects and crime prevention".